IN THE SPECIFICATION:

Please amend the Specification as follows.

Please amend the title as follows:

METHOD AND APPARATUS TO GENERATE PACKET VALIDATION INFORMATION FOR PACKET SECURITY ~~FOR PROTOCOL TRAVERSAL~~

Please replace paragraphs [0005], [0022], [0030], [0047] and [0049] of the specification as follows:

[0005] This invention is related to security and more particularly security protocols to protect user packets. There are currently two main security protocols; Ipsec (Internet Protocol Security, as described, for example, in S. Kent, R. Atkinson, Security Architecture for the Internet Protocol", RFC 2401, November 1998) and SKIP (Simple Key Management for Internet Protocols~~, information is available, for example, from www.skip.org, an overview can be found in http://www.tik.ee.ethz.ch/~skip~/SKIP.html~~).

[0022] Reference C of FIG. 1 denotes a middle node or intermediate node. The node C can have the same structure as the node B, i.e., can be a server or the like, or can be a router. The intermediate nodes are also called middle-box 5 entities ~~(described, for example, in~~

~~http://www.ietf.org/html.charterS/midcOlWcharter.html) in IETF~~. Similar to the receiving node B, also such an intermediate node might need to verify the validity of the message and to make sure that the message was sent from A and was not modified along the way (data origin authentication, integrity protection). Thus, also the intermediate node C includes a validity check function C1, similar as the corresponding validity check function B1 of the node B.

[0030] The field H4 includes the Public Key verification information. This information indicates how the receiving nodes can verify that the Public Key belongs to the claimed entity (i.e., the sending node). This field can e.g. include a Certificate, or just the indication that CGA has been applied (CGA: Cryptographically Generated Address, as described, for example, in Cryptographically Generated Addresses by Tuomas Aura, February 2003~~, (http://www.ietf.org/internet-drafts/draft-aura-cga-OO.txt)~~.

[0047] Another example for a mechanism for preventing replay attacks is the use of nonces. Further applicable anti-replay attack mechanisms are described in document: "On Preventing Replay Attacks on Security Protocols" by Sreekanth Malladi, Jim Alves-Foss, Robert B. Heckendorn, Center for Secure and Dependable Systems, Department of Computer

Science, University of Idaho, Moscow, ID 83844 USA ~~http://www.cs.uidaho.edu/~jima-f/docs/replay02.pdf~~.

[0049] According to the second embodiment, not every single packet will contain the security header. In particular, according to the second embodiment, the security header is added only to some specific packets. Possible applications are Mobile IPv6 and NSIS ~~(Next Steps In signaling, described in http://www.ietf.org/html.charters/nsis-charter.html, for example)~~. In Mobile IPv6 case, in order to allow firewalls to be able to process Mobile IPv6 packets correctly and therefore detect, read and authenticate Binding Update messages without requiring the firewall (FW) and the multiple node (MN) to have a pre-shared security relation, only packets containing Binding Update messages need to have such security header. In case of NSIS signaling used e.g. in the TIST meaning (i.e. to allow a MN to communicate with a firewall without sharing any security association), again only specific packets carrying the signaling will contain the security header. So, the processing of asymmetric encryption is limited to a few elements in the networks and only to a few packets, and not to all packets of the communication.

Please replace the Abstract with the following:

A method for protecting packets to be sent from a first network node to a second network node is provided. ~~According to one embodiment, the~~The method may ~~includes the steps~~ include, for example, ~~of~~ generating validity information for a packet, and generating a header for the packet~~, including~~ which includes the validity information. The method also ~~includes~~ may include ~~the step of~~ sending the packet including the header from the first network node to the second network node. The validity information includes all necessary information required for performing a validity check of the packet. Thus, no pre-established security association is needed to verify the validity of a packet.